REMARKS

The Applicants have amended the claims presently on file to address the issues raised by the Examiner. It is believed that these amendments clearly and patentably distinguish over the art applied by the Examiner and place the application in condition for allowance.

The claims have been redirected to the aspect of the invention described at page 12, lines 13 through 26, namely the fact that the finite field operations are performed on word size representations of the finite field elements and the modular reduction is performed subsequently. Organizing the computations in this manner means that less time is spent reducing the intermediate products and additional protection against DPA type attacks is provided due to the increased computational noise.

Accordingly, claim 1 has been amended to recite upon completion of the computation performed on the machine words, a modular reduction is performed to reduce the result to a predetermined number of words.

Similar language can be found in claim 3 where at step (c)(ii) the processor operates the finite field reducer on the intermediate product to obtain the product of the two elements. The intermediate product is that provided by the word size operation.

Claim 4 has similarly been amended to make it clear that the modular reduction is performed subsequent to the completion of the word size operations on the representations.

With respect to claim 5 it again makes reference to the application of the finite field reducer to the intermediate result.

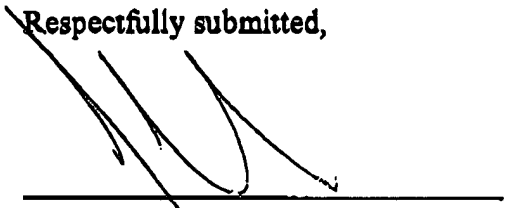
Claim 6 has been amended to specify that the routines used include a finite field operation and subsequent to such operation, a modular reduction.

The Examiner rejected the claims previously on file on the basis of US Patent No. 6,349,318 to Vanstone. The Vanstone reference does not describe the use of word size operations and the subsequent modular reduction. It is clear from column 4, lines 65 through 67 that the partial products formed during the multiplication are reduced prior to their accumulation. This can be contrasted with the example of multiplication provided in the present application where the partial products are accumulated and subsequently upon completion of the accumulation a modular reduction is performed.

Accordingly, it is believed that the application as presently on file clearly and patentably

distinguishes over the art of record and is in condition for allowance.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: March 16, 2006

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/sp